

DHCP SERVER WITH CLIENT AUTHENTICATING FUNCTION AND AUTHENTICATING METHOD THEREOF

Publication number: JP2001211180

Publication date: 2001-08-03

Inventor: MORIYA MASAMI

Applicant: NEC COMMUNICATION SYST

Classification:

- international: H04L9/32; H04L12/28; H04L12/56; H04L9/32;
H04L12/28; H04L12/56; (IPC1-7): H04L12/28;
H04L9/32; H04L12/56

- European:

Application number: JP20000017668 20000126

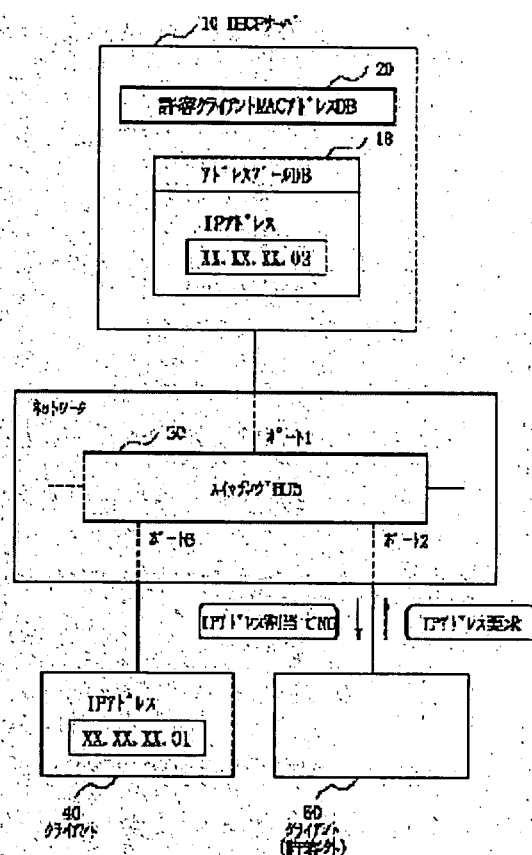
Priority number(s): JP20000017668 20000126

Report a data error here

Abstract of JP2001211180

PROBLEM TO BE SOLVED: To provide high security by equipping a DHCP server with a function of authenticating an IP-address assigned client and releasing an IP address when an unallowed client is found and a function of reporting communication rejection.

SOLUTION: The DHCP server 10 when receiving requests to assign IP addresses from clients 40 and 60 checks whether or not their MAC addresses are registered in an allowed client MAC address DB 20, and allocates and records the IP addresses in an allocated-address DB while making them correspond to the MAC addresses when they are registered. Then an ARP packet is sent periodically to the IP addresses and it is checked whether or not a combination of the transmission source MAC address and the transmission source IP address in its response packet is recorded in the allocated address database, when it is recorded, a regular client is decided and when not, an irregular client is decided.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-211180

(P 2 0 0 1 - 2 1 1 1 8 0 A)

(43) 公開日 平成13年 8 月 3 日 (2001. 8. 3)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード [*] (参考)		
H04L 12/28		H04L 11/00	310	Z	5J104
9/32		9/00	673	B	5K030
12/56		11/20	102	Z	5K033

審査請求 有 請求項の数 7 O L (全 8 頁)

(21) 出願番号 特願2000-17668 (P 2000-17668)

(22) 出願日 平成12年 1 月 26 日 (2000. 1. 26)

(71) 出願人 000232254

日本電気通信システム株式会社
東京都港区三田 1 丁目 4 番 28 号

(72) 発明者 森谷 真佐美

東京都港区三田一丁目 4 番 28 号 日本電気
通信システム株式会社内

(74) 代理人 100082935

弁理士 京本 直樹 (外 2 名)

F ターム (参考) 5J104 AA07 KA02 NA21 PA07

5K030 GA15 HC14 KA02

5K033 AA08 CB08 EC04

9A001 BB02 BB03 BB04 CC06 CC07

DD10 JJ01 JJ18 JJ25 JJ27

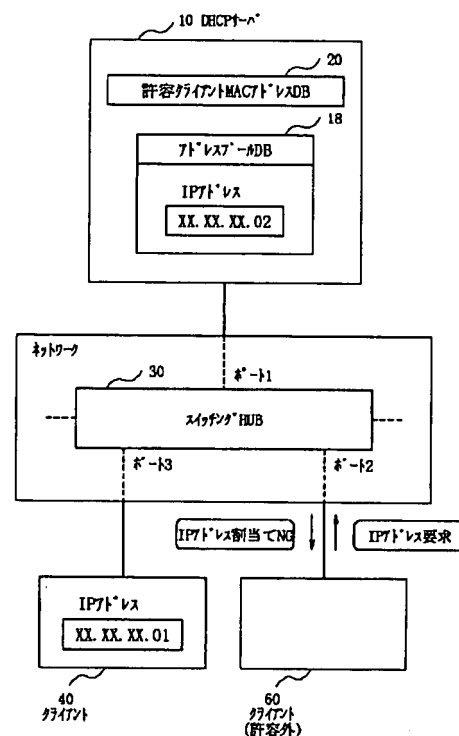
KK56 LL03 LL09

(54) 【発明の名称】 クライアント認証機能付き DHCP サーバ、及びその認証方法

(57) 【要約】

【課題】 DHCP サーバにおいて、IP アドレスの取得希望／取得済みクライアントの正規性を確認する。

【解決手段】 DHCP サーバ 10 は、クライアント 40、60 からの IP アドレスの割当て要求を受けると、その MAC アドレスが許容クライアント MAC アドレス DB 20 に登録されているか照合し、登録されていれば IP アドレスを割当て MAC アドレスと対応付けて割当て済みアドレス DB に記録する。その後、定期的に当該 IP アドレスへ ARP パケットを送信し、その応答パケット中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせが割当て済みアドレスデータベースに登録されているか照合し、記録されていれば正規クライアント、記録されていなければ不正規クライアントと判定する。



【特許請求の範囲】

【請求項 1】 ネットワーク接続されたクライアントからの要求を受け IP アドレスの動的割当てを行う DHCP サーバにおいて、

IP アドレスの割当て許容対象のクライアントの MAC アドレスをあらかじめ登録した許容クライアント MAC アドレスデータベースと、割当て済みの IP アドレスと MAC アドレスとを対応付けて記録するための割当て済みアドレスデータベースとを有し、

クライアントからの IP アドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元 MAC アドレスが前記許容クライアント MAC アドレスデータベースに登録されているか照合し、登録されているときのみ使用可能な IP アドレスを割当てて当該クライアントに通知するとともに、当該 MAC アドレスと対応付けて前記割当て済みアドレスデータベースに登録し、前記 IP アドレスの割当て後、定期的に当該 IP アドレスのクライアントに対して当該クライアントの MAC アドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせが前記割当て済みアドレスデータベースに登録されているか照合し、照合結果に基づいて当該クライアントが正規に IP アドレスを割当てられたクライアントであるか否かを判定することを特徴とするクライアント認証機能付き DHCP サーバ。

【請求項 2】 前記クライアントからの応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合わせが記録されていなければ、当該クライアントが正規に IP アドレスを割当てられたクライアントではないと判定し、当該 IP アドレスの割当てを取消するとともに、当該クライアントに対し強制 IP アドレス解放通知メッセージを送信することを特徴とする請求項 1 記載のクライアント認証機能付き DHCP サーバ。

【請求項 3】 前記クライアントからの応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規に IP アドレスを割当てられたクライアントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該 MAC アドレスに対する通信を行わないよう設定させることを特徴とする請求項 1 記載のクライアント認証機能付き DHCP サーバ。

【請求項 4】 請求項 3 記載のクライアント認証機能付き DHCP サーバとクライアントとを收容し、前記クライアント認証機能付き DHCP サーバからの制御情報を登録する手段と、登録された制御情報に応じて前記クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチ手段とを有することを特徴とする

スイッチングハブ装置。

【請求項 5】 ネットワーク接続されたクライアントからの要求を受け IP アドレスの動的割当てを行う DHCP サーバのクライアント認証方法において、クライアントからの IP アドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元 MAC アドレスが IP アドレスの割当て許容対象のクライアントの MAC アドレスをあらかじめ登録した許容クライアント MAC アドレスデータベースに登録されているか照合し、登録されているときのみ使用可能な IP アドレスを割当てて当該クライアントに通知するとともに、当該 MAC アドレスと対応付けて割当て済みアドレスデータベースに登録し、前記 IP アドレスの割当て後、定期的に当該 IP アドレスのクライアントに対して当該クライアントの MAC アドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせが前記割当て済みアドレスデータベースに登録されているか照合し、照合結果に基づいて当該クライアントが正規に IP アドレスを割当てられたクライアントであるか否かを判定することを特徴とするクライアント認証方法。

【請求項 6】 前記クライアントからの応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合わせが記録されていなければ、当該クライアントが正規に IP アドレスを割当てられたクライアントではないと判定し、当該 IP アドレスの割当てを取消するとともに、当該クライアントに対し強制 IP アドレス解放通知メッセージを送信することを特徴とする請求項 5 記載のクライアント認証方法。

【請求項 7】 前記クライアントからの応答メッセージ中の送信元 MAC アドレス及び送信元 IP アドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規に IP アドレスを割当てられたクライアントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該 MAC アドレスに対する通信を行わないよう設定させることを特徴とする請求項 5 記載のクライアント認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はクライアント認証機能付き DHCP サーバ、及びその認証方法に関し、特にネットワーク接続されたクライアントからの要求を受け IP アドレスの動的割当てを行う DHCP サーバと、その制御の下、クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチングハブ装置と、そのクライアント認証方法とに関する。

【0002】

【従来の技術】DHCP (Dynamic Host Configuration Protocol) はネットワーク内のシステムのIPアドレスを一元管理することができるUDP上のプロトコルで、クライアント/サーバ方式を採用している。通常、DHCPサーバは同一サブネット毎に設置され、クライアントの要求に応じてIPアドレスの動的割当てを行っている。それにより、クライアントは個別にIPアドレスの設定を行うことなく、TCP/IP通信を行うことができる。

【0003】

【発明が解決しようとする課題】しかし、上述した従来のDHCPサーバは、動的割当ての利点がある反面、IPアドレスを割当ての際にクライアントに対しての認証は一切行っていない。そのため、ネットワークに接続してしまえば、どのようなクライアントでもIPアドレスを取得し、通信を行ってしまうことができってしまう。これはセキュリティ上重大な問題である。また、IPアドレスを新規に取得する以外にも、他の正規クライアントのIPアドレスを盗む場合があり、この場合でもクライアントの正規性を確認することができない。

【0004】本発明は、これらの問題を解決するために、DHCPサーバにIPアドレス割当てクライアントの認証及び許容外クライアント発見時のIPアドレス解放通知機能、通信拒否通知機能を具備させることで高いセキュリティを提供する。

【0005】

【課題を解決するための手段】本発明のクライアント認証機能付きDHCPサーバは、ネットワーク接続されたクライアントからの要求を受けIPアドレスの動的割当てを行うDHCPサーバにおいて、IPアドレスの割当て許容対象のクライアントのMACアドレスをあらかじめ登録した許容クライアントMACアドレスデータベースと、IPアドレスとMACアドレスとを対応付けて記録するための割当て済みアドレスデータベースとを有し、クライアントからのIPアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元MACアドレスが前記許容クライアントMACアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なIPアドレスを割当てて当該クライアントに通知するとともに、当該MACアドレスと対応付けて前記割当て済みアドレスデータベースに登録し、前記IPアドレスの割当て後、定期的に当該IPアドレスのクライアントに対して当該クライアントのMACアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせが前記割当て済みアドレスデータベースに登録されているか照合し、照合結果に基づいて当該クライアントが正規にIPアドレスを割当てられたクライアントであるか否かを判定する構成である。

【0006】また、上記構成において、前記クライアントからの応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にIPアドレスを割当てられたクライアントではないと判定し、当該IPアドレスの割当てを取消するとともに、当該クライアントに対し強制IPアドレス解放通知メッセージを送信する構成とすることができる。

10 【0007】あるいは、前記クライアントからの応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にIPアドレスを割当てられたクライアントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該MACアドレスに対する通信を行わないよう設定させる構成とすることができる。

20 【0008】本発明のスイッチングハブ装置は、上記構成のクライアント認証機能付きDHCPサーバとクライアントとを收容し、前記クライアント認証機能付きDHCPサーバからの制御情報を登録する手段と、登録された制御情報に応じて前記クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチ手段とを有する。

30 【0009】本発明のクライアント認証方法は、ネットワーク接続されたクライアントからの要求を受けIPアドレスの動的割当てを行うDHCPサーバのクライアント認証方法において、クライアントからのIPアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元MACアドレスがIPアドレスの割当て許容対象のクライアントのMACアドレスをあらかじめ登録した許容クライアントMACアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なIPアドレスを割当てて当該クライアントに通知するとともに、当該MACアドレスと対応付けて割当て済みアドレスデータベースに登録し、前記IPアドレスの割当て後、定期的に当該IPアドレスのクライアントに対して当該クライアントのMACアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせが前記割当て済みアドレスデータベースに登録されているか照合し、照合結果に基づいて当該クライアントが正規にIPアドレスを割当てられたクライアントであるか否かを判定する工程を有する。

50 【0010】また、上記工程において、前記クライアントからの応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にIPアドレ

スを割当てられたクライアントではないと判定し、当該IPアドレスの割当てを取消すとともに、当該クライアントに対し強制IPアドレス解放通知メッセージを送信する工程を含むことができる。

【0011】あるいは、前記クライアントからの応答メッセージ中の送信元MACアドレス及び送信元IPアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にIPアドレスを割当てられたクライアントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該MACアドレスに対する通信を行わないよう設定させる工程を含むことができる。

【0012】

【発明の実施の形態】まず、本発明の概要を説明する。本発明のクライアント認証機能付きDHCP (Dynamic Host Configuration Protocol) サーバは、IPアドレスの動的割当てを行う場合に発生しうる、なりすましを防止するためのクライアント認証機能を具備し、セキュリティを向上させることを特徴としている。「なりすまし」とは、不正なクライアントが、あたかもネットワーク内の正規のクライアントであるかのようにして、IPアドレスを取得することをいう。

【0013】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0014】図1は本発明の一実施の形態を示すDHCPサーバを用いたネットワークの構成図である。図1を参照すると、サブネット内にDHCPサーバ10が設定され、スイッチングHUB (ハブ装置) 30を含む伝送路を介して接続された複数のクライアント (40及び60のみ図示) に対し、IPアドレスの動的割当てを行っているネットワークである。

【0015】DHCPサーバ10の許容クライアントMACアドレスDB (データベース) 20にはIPアドレス割当てを許容するクライアントのMACアドレスが、アドレスプールDB (データベース) 18には割当て可能なIPアドレス (XX. XX. XX. 02) が記録されている。

【0016】現在、クライアント40は許容クライアントで、そのMACアドレスがDHCPサーバ10の許容クライアントMACアドレスDB 20に記録され、IPアドレス (XX. XX. XX. 01) が割当てられているものとする。クライアント60は許容外のクライアントで、MACアドレスはDHCPサーバ10の許容クライアントMACアドレスDB 20に記録されていない。

【0017】この状態でDHCPサーバ10が、クライアント60からサーバ検索要求を受信した場合、許容クライアントMACアドレスDB 20とクライアント60のMACアドレスとの比較を行う。この比較で一致しな

ければ、DHCPサーバ10はIPアドレスの割当て不能を示すNG情報をクライアント60に送信し、IPアドレスの割当ては行わない。しかし、これで全てのなりすまし防止を行うことはできていない。

【0018】ここで、正規IPアドレスを取得した許容クライアント40の場合を例に、IPアドレスの取得手順を説明する。許容クライアントの認証後、DHCPサーバ10は、ICMP (Internet Control Message Protocol) のEchoメッセージをアドレスプールDB 18から選択したIPアドレス (XX. XX. XX. 01 (この時点ではまだ未使用)) に対して送付する。未使用であることを確認後、アドレスをクライアント40に提示し、クライアント40はそのアドレスを要求する。その後、DHCPサーバ10は正式にIPアドレスの割当てを行う。

【0019】確かにクライアント40は許容クライアントでIPアドレスの割当てでも正常に行われている。しかし、ここで問題が生じる。許容クライアント40がIPアドレスを取得したあとに、そのアドレスを他のクライアントが盗む可能性があるということである。

【0020】それを回避する方法として、定期的に割当て済みの全てのアドレスに対してARP (Address Resolution Protocol) パケットを送付する。その応答によって得られるMAC (Media Access Control) アドレスによりなりすましクライアントを発見することができる。

【0021】そして、実際になりすましクライアントを発見した場合には、DHCPサーバ10は、割当てを認識していないクライアント (例えばクライアント60) に対して強制IPアドレス解放通知を送付する。

【0022】しかし、この強制IPアドレス解放通知は通知のみで、IPアドレスの解放はクライアント側に依存してしまう。そのため、実際に解放されることはまず無いと考えた方がよい。

【0023】よって、入出力ポート間でMACアドレスによるパケットデータのスイッチングを行うスイッチング手段 (図示せず) を有するスイッチングHUB 30に以下の機能を具備させることで、なりすましクライアントのIP通信を停止させる。

【0024】ARP応答にて許容外MACアドレスが存在する場合に、DHCPサーバ10は、なりすましクライアント60の通信拒否をスイッチングHUB 30に通知する。そして、スイッチングHUB 30は、内蔵する制御情報受信登録手段 (図示せず) により、DHCP 10からの通知情報を抽出し内蔵するMACアドレス/ポート番号対応テーブル (図示せず) 内にあるクライアント60のMACアドレス通信可否状態 (フラグ) をNG (通信否) とする。これにより、スイッチングHUB 30は通信可否状態がNGのクライアント60に対するスイッチング手段によるスイッチング動作を停止しその通

信を停止させる。

【0025】次に、DHCPサーバ10の詳細構成を図2に示す。

【0026】図2において本例のDHCPサーバ10は、IPアドレス割当てを許容するクライアントのMACアドレス（複数可）を記録しておく許容クライアントMACアドレスDB（データベース）20と、通常の動的IPアドレス割り当てを行うDHCPサーバ処理部16と、その割当て状況（IPアドレスとMACアドレスとの組合せ）を記録しておく割当て済みアドレスDB（データベース）17と、現在、使用されているIPアドレス状況を確認する割当てアドレス確認部12と、その使用状況を記録しておく使用アドレスDB（データベース）19と、状況確認後、許容外クライアントが検出された場合にそのクライアントに対してアドレスの解放を促すアドレス解放通知部13と、許容外クライアントの通信を停止させる通信拒否通知部14と、それぞれのデータの送受信する際の全般的な処理を行う通信処理部15と、まだ割当てられていないアドレスを記録しているアドレスプールDB（データベース）18とから構成される。

【0027】許容クライアントMACアドレスDB20には、予めIPアドレス割当てを許容するクライアントのMACアドレスが設定されている。これにより、クライアントからのサーバ検索要求受信時、そのMACアドレスとDB内に設定されているMACアドレスを比較し、認証を行う。なお、許容クライアントMACアドレスDB20のMACアドレス登録内容（MACアドレス）は、運用状態に応じて適宜書き換えられる（管理者等による）。すなわち、常に最新のIPアドレス割当てを許容するMACアドレス情報が得られる。

【0028】DHCPサーバ処理部16により割当てられたIPアドレスは、対応するMACアドレスとともに割当て済みアドレスDB17に記録される。割当てアドレス確認部12は、IPアドレス割当て要求受付時に、アドレスプールDB18から選択した割当て予定IPアドレスに対して、使用状況を確認するため、ICMP_Echoメッセージ（図3参照）を送付する。この使用状況は使用アドレスDB19に記録される。

【0029】許容クライアントに割当てられたIPアドレスが許容外のクライアントに使用されるのを防止するために、IPアドレス割当て後、定期的に、ARPパケット要求/応答メッセージ（図4参照）によって対応するMACアドレスによって検出する。それによって得られるデータ（IPアドレスとMACアドレスとの組合せ）は、割当てアドレス確認部12の一時的なメモリ内にARPテーブルとして登録される（図5参照）。このARPテーブルと、割当て済みアドレスDB17、許容クライアントMACアドレスDB20とが比較され判別される。許容クライアントMACアドレスDB20によ

り、そのMACアドレスが現在、許容されているか判定され、割当て済みアドレスDB17により、MACアドレスとIPアドレスとの組み合わせが正しいか判定される。

【0030】実際に許容外のクライアントがIPアドレスを使用していた場合には、アドレス解放通知部13及び通信処理部15により強制IPアドレス解放通知がそのクライアントに対して行われ、許容外クライアントの情報は使用アドレスDB19の許容外クライアント情報部分に記録され、その後、割当ては行わない。

【0031】許容外クライアント検出時、通信拒否通知部14は、ネットワーク内のスイッチングHUB30に、通信拒否通知を送信する。通信拒否通知を受けたスイッチングHUB30は、内蔵するMACアドレス/ポート番号対応テーブル内の通信可否状態（フラグ）にNG（通信否）を設定する（図6参照）。

【0032】次に、図1～図6とともに、動作シーケンスを示す図7を参照して本実施の形態の動作についてさらに詳細に説明する。

【0033】前提条件として、サブネット内にDHCPサーバ10が設置され、登録された許容クライアントMACアドレスは“AA AA AA AA AA A”とする。そして、許容クライアントをクライアント40（MACアドレス：AAAA AA AA AA AA）、許容外クライアントをクライアント60（MACアドレス：BB BB BB BB BB BB）とし、共にIPアドレスが設定されていない状態（状態401、状態601）とする。なお、スイッチングHUB30のポート1にDHCPサーバ10、ポート2にクライアント60、ポート3にクライアント40が、それぞれ適切なネットワーク経路を介して接続されている。

【0034】正当なクライアントであるクライアント40は、ネットワークアドレスを構築するために、DHCPサーバ10に対してDHCP_DISCOVERメッセージをブロードキャストする。

【0035】DHCPサーバ10は、クライアント40からのメッセージ中の送信元MACアドレス（AA AA AA AA AA AA）が、保持している許容クライアントMACアドレス（複数可。この場合、AA AA AA AA AA AA）中にあるか照合する。照合の結果、許容クライアントであれば、DHCPサーバ10は割当て予定のIPアドレスに対して、ICMP_EchoメッセージにてIPアドレスの使用状況を確認し、未使用であればそのIPアドレスを設定した構成情報をDHCP_OFFERメッセージにてクライアント40に通知する。

【0036】通知を受けたクライアント40は、サーバIDなどを設定してDHCP_REQUESTメッセージをブロードキャストする。クライアント40によって選択されたDHCPサーバ10は、IPアドレス（例え

ば、“10. 1. 32. 1”)を指定してクライアント40に対してDHCP__ACK (OK) メッセージを送信する。

【0037】ただし、割当てするIPアドレスがない等の要因で割当て不可能の場合は、DHCP__NAK (NG) メッセージが送信され、割当ては行われない。この時点でクライアント40は、電源がまだON状態であり、DHCPサーバ10とのメッセージ送受信が可能である。これを状態402とする。

【0038】一方、不正なクライアントであるクライアント60 (MACアドレス:BBBB BB BB BB) が、DHCP__DISCOVERメッセージによりIPアドレス割当て要求を行うと、DHCPサーバ10は、クライアント40に対して行ったと同様に、MACアドレスによる許容クライアント判定を行う。しかし、クライアント60は許容外のクライアントであるためDHCPサーバ10は許容外クライアント通知を送信し、IPアドレス割当ては行わない。これを状態602とする。

【0039】IPアドレス取得を失敗した許容外クライアント60 (そのユーザ) は、正当なIPアドレス割当てを受けているクライアント40になりすますため、クライアント40の電源をOFFし動作不能状態 (状態403) とし、自己のIPアドレスとしてクライアント40のIPアドレス (“10. 1. 32. 1”) を設定する。これを状態603とする。

【0040】一定時間経過後、サーバ管理者によって設定された時間毎に、DHCPサーバ10は、ARP要求メッセージをネットワーク上にブロードキャストする。

【0041】クライアント40は電源がOFFされているため、ARP応答メッセージはクライアント60からのみ返却される。

【0042】このARP応答メッセージに含まれるIPアドレスとMACアドレスの組合せ (ARPテーブル) に対して、割当て済みアドレスDB17、許容クライアントMACアドレスDB20で保持しているデータとそれぞれ照合する。照合の結果、該当IPアドレス (この場合、“10. 1. 32. 1”) に対して違うMACアドレス (この場合、“BB BB BB BB BB BB”) が存在した場合には、ARP応答メッセージを返送したクライアント (クライアント60) は許容外クライアントであるとして、そのMACアドレス (“BB BB BBBB BB BB”) に対して、アドレス

解放通知部13より強制IPアドレス解放通知メッセージを送信する。

【0043】解放通知メッセージ送信後、DHCPサーバ10は、通信拒否通知部14よりスイッチングHUB30に対して通信拒否通知メッセージを送信し、スイッチングHUB30内のMACアドレス/ポート番号対応テーブル内の該当するMACアドレス (“BB BB BB BB BB BB”) の通信可否状態をNGとして通信が行われないようにする (図6参照)。これにより、なりすましクライアント (正当なクライアント40になりすましたクライアント60) のIP通信を停止させることができる。この状態を状態604とする。

【0044】

【発明の効果】本発明によれば、DHCPサーバによりIPアドレスの動的割当てを行っているネットワークにおいて、許容クライアント認証機能及び定期的なARPパケット送付により、クライアントに割当てたIPアドレスに対応するMACアドレス状況を確認し、許容外クライアントを発見した場合の対処機能としてIPアドレス解放通知機能、通信拒否通知機能及び通信拒否手段を具備することで、許容外クライアントのなりすましを防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態を示すネットワーク構成図である。

【図2】DHCPサーバの詳細構成を示すブロック構成図である。

【図3】ICMP__Echoメッセージの構成例を示す図である。

【図4】ARPパケット要求/応答メッセージの構成例を示す図である。

【図5】ARPテーブルの構成例を示す図である。

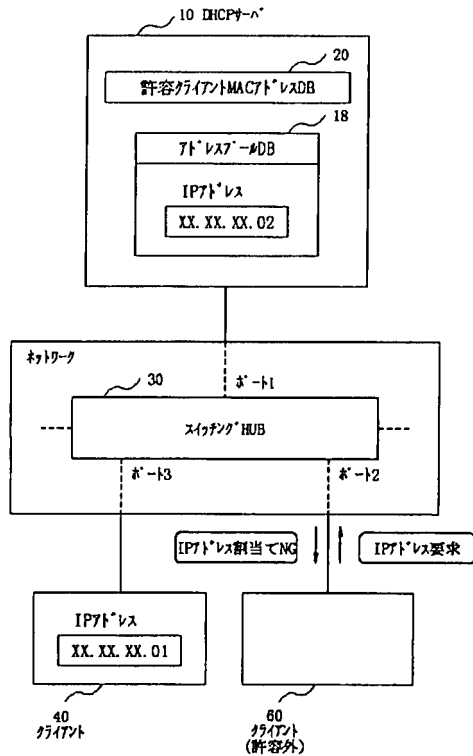
【図6】MACアドレス/ポート番号対応テーブルの構成例を示す図である。

【図7】本発明の一実施の形態の動作シーケンスを示す図である。

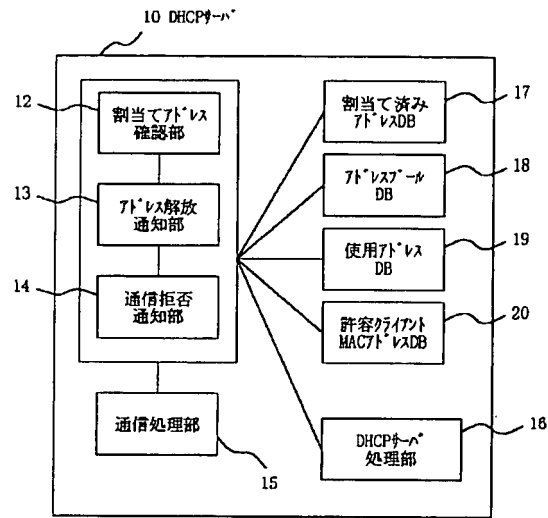
【符号の説明】

10 DHCPサーバ
17 割当て済みアドレスDB
18 アドレスプールDB
20 許容クライアントMACアドレスDB
30 スwitching HUB
40, 60 クライアント

【図1】



【図2】



【図3】

【図3】

ICMP (Echo) メッセージフォーマット

タイプ	コード	チェックサム
識別子	シーケンス番号	
データ		

【図4】

ARPパケットフォーマット

ハードウェアタイプ		プロトコルタイプ
プロトコルアドレス長	ハードウェアアドレス長	要求or応答
送信元MACアドレス		
送信元IPアドレス		
ターゲットMACアドレス		
ターゲットIPアドレス		

ARPテーブル

IPアドレス	MACアドレス
AA. BB. CC. DD	EE FF GG HH II JJ
.	.
.	.
.	.

【図 6】

MACアドレス/ポート番号対応テーブル

MACアドレス	ポート番号	通信可否状態
BB BB BB BB BB BB	02	NG
.	.	.
.	.	.
.	.	.

【図 7】

